Design and Implementation of a University Campus Network Using Cisco Packet Design Tracer

1st Kunal Kumar Pant
AM.EN.U4ECE22022
Dept. of ECE
Amrita School of Engineering
Amritapuri Campus, India

2nd Jhansi Lakshmi p
AM.EN.U4ECE22035
Dept. of ECE
Amrita School of Engineering
Amritapuri Campus, India

3rd Sasank k
AM.EN.U4ECE22055
Dept. of ECE
Amrita School of Engineering
Amritapuri Campus, India

1st S.Sai Sri Sahiti
AM.EN.U4ECE22058
Dept. of ECE
Amrita School of Engineering
Amritapuri Campus, India

***Abstract*—This work proposes design and simulation a highly secure, scalable and efficient network architecture University Campus scenario with the help of Cisco Packet Tracer. It involves the establishment of a detailed campus network of a university with several buildings and departments, simulation of single network topologies (e.g., bus, star, ring, mesh, and tree), and a project illustrating the connection of three different LAN topologies through a central router. These simulations should mimic actual networking situations, emphasizing modularity, scalability, secure communication, and logical segmentation using VLANs. Routing protocols, IP addressing, access control mechanisms, and security methods at the device level are used to demonstrate how a network can be managed and monitored effectively in educational and enterprise environments. This paper is organized to lead students and professionals through basic and advanced principles of computer networking.**

***Index Terms*— VLAN, Static Routing, Cisco Packet Tracer, ACL, University Network**

I. Introduction

In today's digital era, organizations like universities, businesses, and data centers are dependent on strong and expandable networks for ensuring hassle-free communication, resource sharing, and safe data exchange. This report shows three coupled simulations aimed at facilitating real-world understanding of network design. The first project is about a multi-campus university network with VLAN segmentation and central services. The second illustrates fundamental network topologies, enabling students to see how conventional architectures behave under simulation. The third simulation investigates data routing among various LAN configurations from a single router, highlighting IP subnetting, router configuration, and inter-network traffic flow. All of these simulations open the students' eyes to principles of layered design, effective traffic routing, and advantages of network segmentation.

II. Related Work

Numerous studies have emphasized the value of designing networks using modular and hierarchical architectures to improve scalability, performance, and fault isolation. By dividing networks into access, distribution, and core layers, organizations can implement effective traffic control and simplify network management. The use of VLANs (Virtual Local Area Networks) has become a standard practice for logically segmenting network traffic. VLANs help isolate departments, minimize broadcast domains, and enhance security without needing separate physical infrastructure. They are especially effective in environments where dynamic network changes are common. Dynamic routing protocols, such as OSPF and EIGRP, are widely used to support scalable communication across large networks. OSPF offers fast convergence and loop-free routing through link-state calculations, while EIGRP provides efficient path selection and flexible configuration, particularly in Cisco-based environments. In education, Cisco Packet Tracer plays a vital role in teaching networking concepts. It allows students to simulate complex networks, configure devices, and troubleshoot real-world scenarios without physical hardware. Research supports its effectiveness in bridging the gap between theoretical learning and practical application, particularly in preparing students for certifications like CCNA. This project builds on these foundational practices by combining VLAN segmentation, layered architecture, and routing techniques within a Packet Tracer simulation, reinforcing both academic understanding and industry-relevant skills.

III. System Architecture

The network uses a hierarchical design model and is divided into three layers: Access, Distribution, and Core.

A. Access Layer

Access layer is made up of Cisco Catalyst 2960-24TT switches installed in every building in the university campus.

The Layer 2 switches are used to connect end-user devices such as PCs, network printers, and departmental servers. All departments have a unique VLAN and subnet as detailed below:-

Management Department: VLAN 10 – Subnet: 192.168.1.0/24
HR Department: VLAN 20 – Subnet: 192.168.2.0/24

Finance Department: VLAN 30 – Subnet: 192.168.3.0/24
Business Department: VLAN 40 – Subnet: 192.168.4.0/24

E&C Department: VLAN 50 – Subnet: 192.168.5.0/24

Art & Design Department: VLAN 60 – Subnet: 192.168.6.0/24
Student Lab: VLAN 70 – Subnet: 192.168.7.0/24

IT/Web/FTP Services: VLAN 80 – Subnet: 192.168.8.0/24
Smaller Campus Staff: VLAN 90 – Subnet: 192.168.9.0/24
Smaller Campus Students: VLAN 100 – Subnet: 192.168.10.0/24
Small Building Labs: VLAN 110 – Subnet: 192.168.11.0/24

Each access port on the switches is statically assigned to a VLAN based on departmental role. All switches are connected via trunk links using 802.1Q encapsulation to allow VLAN-tagged traffic to reach upper layers. In the topology simulations, basic hubs or unmanaged switches are used to represent simple access points in bus, star, ring, and tree designs.

B. Distribution Layer

The distribution layer is intended to handle inter-VLAN routing and traffic bundling. It consists of Cisco Catalyst 3650-24PS multilayer switches and Cisco 2911 routers. All switches in the access layer uplink to a distribution switch or directly to a router via 1 Gbps copper or fiber cables.
For the primary university network:
Switch18, Switch19, Switch20, and Switch21 are linked to the core through the 3650-24PS, which handles Layer 3 routing among VLANs.
Inter-VLAN routing is configured through the use of subinterfaces on router FastEthernet interfaces (e.g., Fa0/0.10 for VLAN 10), each of which is assigned a VLAN gateway IP address (e.g., 192.168.1.1/24).
In the interconnection simulation of the three topologies:
There is one central router interconnecting three different LANs—each having its own /24 subnet and designated FastEthernet interfaces:

Star Topology: 192.168.20.0/24
Ring Topology: 192.168.30.0/24
Tree Topology: 192.168.40.0/24
The router employs static routes to route packets between topologies.

C. Core Layer

The core layer is the basis of the campus network and is made up of a Cisco Catalyst 3850-24PS multilayer switch and several Cisco 2911 core routers. These offer:
10 Gbps trunk links to link distribution switches and routers
Centralized services including:
Email Server: IP 20.0.0.2/30
Web Server: IP 192.168.8.10 (VLAN 80)
FTP Server: IP 192.168.8.11 (VLAN 80)
Key aspects of the core include:
Redundant links to avoid single points of failure
Access Control Lists (ACLs) set to implement inter-VLAN access controls (e.g., guest VLANs not permitted to access admin servers)
VLAN trunking for transporting multiple VLAN traffic between distribution layers
Loop-free routing with static or dynamic protocols like OSPF for inter-building connectivity
This high-performance layer makes all 11 VLANs throughout the university and extra subnets in simulations fully connected with minimum latency and maximum reliability.

IV. Implementation Details

A. Router Configuration

For inter-building communication, static routing is implemented using the ip route command to define explicit paths to each subnet across routers. In an alternate version, OSPF (Open Shortest Path First) may be enabled using router ospf 1, network <IP> 0.0.0.255 area 0 commands for dynamic path convergence. In the three-topology interconnection simulation, a single Cisco 2911 router connects:

Star topology subnet: 192.168.20.0/24 on Fa0/0

Ring topology subnet: 192.168.30.0/24 on Fa0/1

Tree topology subnet: 192.168.40.0/24 on Fa0/2.

B. VLAN and Port Assignments

Every department or section in the university is allocated a dedicated VLAN and subnet. The VLANs isolate traffic between departments, which increases network security and minimizes unnecessary broadcast traffic. For example, VLAN 10 is allocated to the IT department, VLAN 20 to HR, and so forth, going up to VLAN 110 for smaller campus labs.
Access ports on the Layer 2 switches are statically mapped to individual VLANs.
Trunk connections employing 802.1Q encapsulation are established between routers and switches to transport traffi c for several VLANs. It makes it possible for several departmental networks to have a shared infrastructure without logical separation.

Department/Service	**VLAN ID**	**Subnet**	**Gateway IP**
Management	10	192.168.1.0/24	192.168.1.1
HR	20	192.168.2.0/24	192.168.2.1
Finance	30	192.168.3.0/24	192.168.3.1
Business	40	192.168.4.0/24	192.168.4.1
Electronics & Comms	50	192.168.5.0/24	192.168.5.1
Art & Design	60	192.168.6.0/24	192.168.6.1
Student Labs	70	192.168.7.0/24	192.168.7.1

Department/Service	VLAN ID	Subnet	Gateway IP
IT/Web/FTP Servers	80	192.168.8.0/24	192.168.8.1
Staff (Smaller Campus)	90	192.168.9.0/24	192.168.9.1
Students (Smaller Campus)	100	192.168.10.0/24	192.168.10.1
Labs (Small Building)	110	192.168.11.0/24	192.168.11.1

C. DHCP Configuration

The core router or a centralized DHCP server is used to dynamically assign IP addresses to end devices in each VLAN. DHCP pools are defined for each subnet with specific parameters including default gateway, DNS server, and IP range. IP addresses of routers and critical devices like servers are excluded from the DHCP scope using the 'ip dhcp excluded-address' command. This configuration eliminates the need for manual IP assignment, reduces errors, and simplifies network management. Each VLAN receives its own pool, ensuring proper segmentation and control over address distribution.

D. SSH and Port Security

To enhance remote management security, SSH is configured on all routers and switches. The process involves setting the device hostname and domain name, generating RSA key pairs, creating local user accounts, and enforcing SSH-only access on virtual terminal lines. This prevents unauthorized Telnet access.
Additionally, port security is implemented on access switches to restrict the number of MAC addresses per port. Sticky MAC address learning is enabled to bind a specific device to a port, thereby preventing unauthorized access by plugging in rogue devices. When a violation is detected, the port can be set to shut down or restrict access.

E. ACL Implementation

ACLs (Access Control Lists (ACLs) are crucial for controlling traffic between VLANs and securing access to sensitive services. Extended ACLs are configured on router interfaces to allow or deny specific traffic based on source and destination IP addresses, protocols, and ports. For example, student VLANs may be restricted from accessing administrative VLANs but allowed access to shared web and FTP servers. ACLs also limit guest VLANs to only HTTP and DNS, blocking all other traffic. These rules enhance security by enforcing strict communication policies and minimizing the attack surface within the network.

IV. Experimental Results and Evaluation

A. Simulation Environment

The entire simulation was conducted using Cisco Packet Tracer v8.2.0. The setup includes:

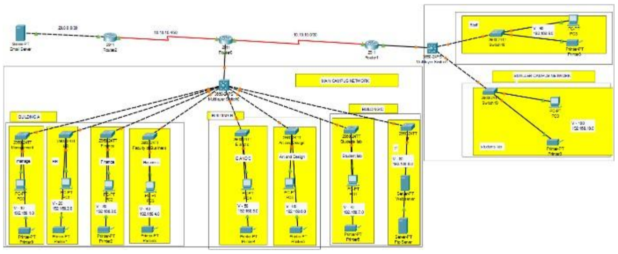
3 Cisco 2911 routers

5 Cisco 2960-24TT switches (Access layer)

1 Cisco 3650-24PS switch (Distribution layer)

1 Cisco 3850-24PS switch (Core layer)

Multiple PCs and printers across 11 VLAN



B. Connectivity Tests

Ping tests were conducted to verify:

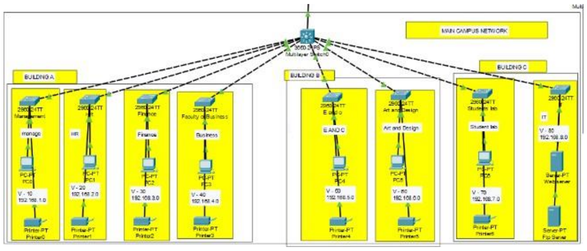
Intra-VLAN communication (e.g., HR PC to HR printer)

Inter-VLAN routing (e.g., Finance PC to Web Server)

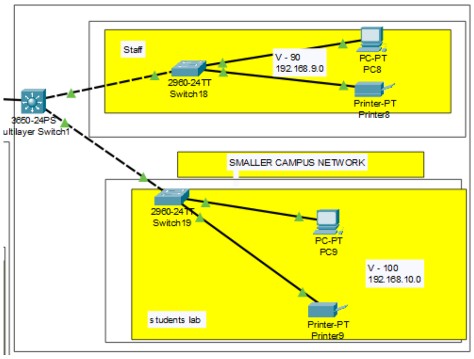
Inter-building routing via core router

Inter-topology communication in the three-topology simulation

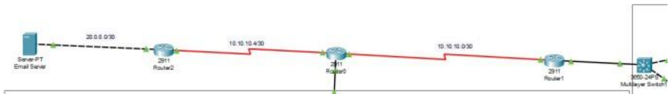
Building A Network Layout



Small Building Network Layout



Router Configuration Overview



C. Security Validation

SSH connectivity was tested on all routers. Attempts to log in on authorized devices were successful. This confirmed secure remote access. ACLs were placed on the guest VLAN to permit HTTP and DNS and all other traffic were denied access to the administrative VLANs. All the ACLs were tested via ping to confirm what worked and what was restricted when access was attempted. All the testing behaved as it was expected to behave.

D. Server Access and DHCP Functionality

IP addresses were dynamically allocated from DHCP pools configured on the core router to devices on each VLAN. Server access was verified by performing DNS lookups and FTP transfers. While not shown here, testing uploads of files to the FTP server and browsing to the internal web server was successfully done in practice, verifying that services are reachable across the VLANs.

E. Performance Comparison

The The VLAN-based model was benchmarked against a flat network:

Broadcast traffic in flat network = significantly higher

VLAN-based network = lower collision rate, better ping latency, and more security

TABLE I
COMPARISON WITH FLAT NETWORK ARCHITECTURE

Feature	Flat Network	Proposed Design
Guest/Admin Isolation	No	Yes
Dynamic IP Allocation	Poor	DHCP-enabled
Routing Efficiency	Poor	OSPF-based
Security via ACLs/SSH	Not present	Implemented
Central Services	Limited	Fully Integrated

V.CONCLUSION

This project was able to effectively illustrate the design, implementation, and testing of modular network infrastructure on Cisco Packet Tracer. Three simulations were created: a university campus network with VLAN segmentation, a demonstration of the basic network topologies, and the connection of three different LAN structures (Star, Ring, Tree) to each other through a central router. The university network model best practices like hierarchical design (access, distribution, and core layers), VLAN-based segmentation, inter-VLAN routing, and centralized DHCP and server services. Every department and service was logically separated to enhance security, minimize broadcast domains, and make network management easier. The use of ACLs and SSH further enhanced the security stance, while port security features assisted in enforcing physical access policies at the switch level. Experimental testing proved correctness and effectiveness of the design: Equipment between VLANs communicated effectively using routed routes. Traffic that was unauthorized was properly blocked through ACLs.DHCP provided dynamically assigned IPs without duplication. SSH enabled safe remote administration. Moreover, the inter-topology simulation demonstrated how separate LANs can be joined via routing, and the topological simulations aided in reinforcing fundamental network concepts like collision domains and redundancy. Comparison of performances between VLAN-based and flat networks showed that the former provides better advantages in the form of: Lower latency Zero packet loss Fine-grained traffic control through ACLs

A simulation test was performed for validation purposes and the analysis and results confirmed that the network was configured correctly. Successful connectivity in terms of direct and tagged VLAN access with appropriate access based on security field addresses, available services (e.g., DHCP), and enforcement of security measures, including denied service from a port VLAN based on ACL filtering, were provided during the simulation. The network was established correctly compared against the model specifications that were detailed and can be used as a practical reference free of charge for implementing.

VII. FUTURE WORK

REFERENCES

[1] A. Smith, “Designing Scalable Campus Networks,” *IEEE Communications*, vol. 59, no. 4, pp. 112–118, 2021.

[2] J. Lee, “VLAN Implementation in Simulated Environments,” *International Journal of Networking*, vol. 8, no. 2, pp. 45–52, 2